EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., Plaintiffs, v. BRAD RAFFENSPERGER, ET AL., Defendants.	CIVIL ACTION FILE NO. 1:17-cv-2989-AT

DECLARATION OF S. MERRITT BEAVER

Pursuant to 28 U.S.C. § 1746, S. MERRITT BEAVER, Chief Information Officer in the office of the Secretary of State for the State of Georgia, declares as follows:

1. I make this Declaration in support of a response by Defendant Brad Raffensperger ("Secretary Raffensperger"), in his official capacity as Secretary of the State of Georgia and as Chair of the State Election Board of Georgia; David J. Worley, Rebecca N. Sullivan, Ralph F. Simpson, and Seth Harp, in their individual capacities and as members of the State Election Board ("State Board Members"); and the State Election Board of Georgia ("State Board") (collectively, the "State

Defendants") to the motion for a preliminary injunction in the above-styled matter of Donna Curling, et al., v. Brad Raffensperger, et al. (Civil Action No. 1:17-cv-2989-AT).

2. I am the Chief Information Officer for the Office of the Georgia Secretary of State and have held that position since January 2014. I have over twenty-five years of experience in software and information technology with special attention to information privacy. I have had numerous information technology ("IT") roles in the healthcare industry focused on protecting patient information, including with McKesson, GE Medical, and HealthPort. I have a Six Sigma Black Belt certification in process improvement that I earned while I was at General Electric. I have a BS in Electrical Engineering from Virginia Tech and an MBA from Keller Business School.

3. I write this affidavit to explain the efforts the Secretary of State's office has taken to increase the security of Georgia's elections systems since Logan Lamb and others were allegedly able to access voter information hosted on the "elections.kennesaw.edu" server in or around August of 2016. What follows is a list of measures the Secretary of State's office has taken to increase security since that time.

Changes to the Center for Election Services

4. Since the alleged access at KSU, the Secretary of State's office has made substantial changes to the security surrounding the Center for Election Services ("CES").

5. It has established a multi-tiered security environment, including monitoring support from the Department of Homeland Security ("DHS"), the Multi-State Information Sharing & Analysis Center ("MS-ISAC"), and two different private sector security monitoring firms.

Additionally, it has transitioned the CES into the Secretary of State's network, which is monitored every hour of the day and all days of the year. This includes added video security surveillance of the air-gapped area of Georgia's servers that house election data.

6. The Secretary of State's office now requires an annual cyber security assessment for the CES.

7. Further, the Secretary of State's office has established endpoint protection on all computer servers and desktops in the CES that are not in the air-gap environment.

8. It has implemented fully-monitored-and-managed firewall protection of all networks that are not in the air-gapped environment.

9. The Secretary of State's office has established network segmentation to limit access to secure networks to only those individuals with "Need Access" privileges.

10. It has utilized DHS weekly vulnerability scanning of all internet connected networks to identify vulnerabilities accessible to external bad actors and has engaged DHS for physical security assessments for local election offices and warehouses.

11. The Secretary of State's office has implemented policies and procedures for CES that mirror the Secretary of State's policies and procedures.

New Security for Ballot Building and ExpressPoll

12. The Secretary of State's office has moved all ballot building and ExpressPoll data set production to the Secretary of State's office.

13. The Secretary of State's office has established a new hardened air-gapped, Secretary of State IT-managed network which houses both the GEMS ballot building process and the ExpressPoll data set production.

14. The Secretary of State has updated its GEMS database transmittal procedure. To transmit the GEMS database, the password protected file is zipped, encrypted and placed on a Secretary of State watermarked CD. In order to obtain the encryption key to access the password protected file, a specific individual documented as the county contact in each county election office must call the Secretary of State's office and provide a verification code for the SOS watermarked CD. After the information provided by the county contact is validated, the Secretary of State's Office releases the encryption key to the county.

15. Additionally, now all watermarked ballot proofs and database structure reports prepared for each county are in PDF format only and placed within a county specific folder on a Secretary of State IT managed and secured file transfer protocol ("SFTP") site. These files are automatically removed after 60 days.

16. Likewise, the only non-PDF files made available to counties through the Secretary of State's SFTP site are ExpressPoll Logic and Accuracy testing, ExpressPoll absentee, and ExpressPoll bulk update data sets. The Logic and Accuracy testing set contains only a subset of voters and includes no personal identifying information. The absentee data set contain no voter information and the bulk update file only contains a list of voter registration IDs. These files are also automatically removed from the SFTP site after 60 days.

17. The Secretary of State's office has further protected ExpressPoll Election Day data. For instance, all ExpressPoll Election Day files containing the full list of voters for an election are placed in locked bags and physically delivered and picked up from counties by Secretary of State Investigators.

Updated ENET Security

18. State Defendants also conducted parallel testing on election day where a copy of an actual county GEMS database is used with a voting machine set up in the Secretary of State's office and set in election mode for a specific real county precinct.

Ballots are entered hourly and videotaped to verify accuracy of the system at the end of the day. The equipment is set to mimic just what is in use at the precinct that day.

19. The Secretary of State's office has ensured that login access to ENET now requires a multifactor authentication.

20. The office has also implemented other security methods, including expiring passwords, anti-brute force software, and mandatory time-outs for ENET use.

21. The Secretary of State's office also performs a complete audit of ENET users at least annually, users are automatically moved to inactive status after seventy-five (75) days of inactivity. An administrator must move an inactive user from inactive to active.

Additional Security Measures

22. The Secretary of State hascomprehensively increased its security measures, which impacts the overall ability to access Georgia's voter information.

23. It has installed "Albert sensors" in the Secretary of State network, which detect traffic coming into and out of a computer network.

24. It has ensured that Secretary of State employees must both establish complex, sixteen (16) character passwords to access the internal network and complete cyber-defense training.

25. Additionally, the Secretary of State's office now uses Cloudflare for network security to monitor and block external attempts to breach the Georgia Voter Registration System using methods like SQL injection or cross site scripting.

26. The Secretary of State's office employs an external source for complete independent penetration testing of our connected network environment.

27. The Secretary of State's office has joined several organizations that provide security election support and monitoring: MS-ISAC, Election Infrastructure Information Sharing & Analysis Center ("EI-ISAC"), and Electronic Registration Information Center ("ERIC").

28. The Secretary of State has encouraged Georgia counties to also join EI-ISAC, of which over sixty (60) counties have.

29. State Defendants have attended, and continue to attend, confidential security briefings from DHS as well as election security workshops and conferences.

30. The Secretary of State's office has participated in multiple nationwide election security tabletop exercise, which provide real life exercises to demonstrate cyber-attack examples and how to work through them.

31. All of these measures are aimed to increase the security of Georgia's voter information and prevent any unlawful access to Georgia's election system.

I declare under penalty of perjury that the foregoing is true and correct to the best of my ability.

Executed this 9th day of July, 2019.

S. MERRITT BEAVER
Chief Information Officer in the office of the Secretary of State for the State of Georgia